Information security burnout: Identification of sources and mitigating factors from security demands and resources

Cong Pham, H

10.1016/j.jisa.2019.03.012
Journal of Information Security and Applications
Elsevier

Information Security Burnout: Identification of Sources and Mitigating Factors from Security Demands and Resources

ABSTRACT

This study examines how information security burnout can develop from complying with organisational security demands, and whether security burnout can be reduced by engaging organisational and personal resources. The Job Demands-Resources model was extended to the IT security context, to develop and empirically test a security burnout model, using a sample of 443 participants in Vietnam. The results demonstrate that security task overload and difficult access to security requirements increased security burnout while dealing with challenging security requirements reduced burnout. Neither organisational resources nor user self-efficacy were effective in reducing burnout. Moreover, simple security tasks did not guarantee a burnout-free experience for users. The findings emphasise the significance of providing resources and designing security tasks as challenging and rewarding experiences, rather than ~~just~~ simply reducing user involvement as a source of decreasing cyber security risks. The research establishes a theoretical basis for further studying the phenomenon of security burnout and its role in user security management.

Key words: security, human factors, security stress, technology stress, compliance fatigue, IT competency

1. Introduction

Due to rapid deployment of networked enterprise information systems, risks to organisations' information resources are growing. Loss of sensitive information due to the ease of access to information online continues to be a major concern for businesses (Li et al., 2014). Organisations often implement technical and administrative measures to protect their digital resources and physical IT assets (Johnston et al., 2015). A key objective of employing administrative measures, such as policies and procedures as well as education and training, is to guide and encourage employees to follow safe security practices (e.g. to not share passwords or check suspicious email attachments before opening them). In fact, a majority of organisational security problems are indirectly caused by employees who violate or neglect the IT policies of their organisations (Warkentin et al., 2007). In order to maintain an effective IT system in an ever-changing cyber-security landscape, organisations require ongoing security compliance from employees (Renaud and Flowerday, 2017). Thus, employee compliance activities are critical (Warkentin and Willison, 2009) when it comes to maintaining a safe cyber system. However, users' low motivation to follow security policies leads to more than 40% of security breaches (Johnston et al., 2015).

There has been previous behavioural security research that examines the actors that affect employees' security practice at work (Crossler et al., 2013). Others have considered security compliance as a rule-following behaviour, where sanctions and rewards for compliance behaviour were explored (Herath and Rao, 2009a; Hu et al., 2011). Additionally, security compliance may be the result of users' strategies applied in order to reduce fear of the consequences of security risks. Protection Motivation Theory (PMT) has been employed to explain these types of user responses to cyber risks (Herath and Rao, 2009b; Vance and Siponen, 2012). PMT theorises that the need to protect oneself (protection motivation) mediates the impact of threat and coping appraisal on protective intentions or behaviours (Maddux and Rogers, 1983). For example, a person's intention to comply with security policies would be influenced by ~~the~~ combination of the perceived severity of the threat, perception of ~~vulnerability with regard~~ to risks, ~~users'~~ ability to respond (response efficacy), cost of response, and self-efficacy (self-belief in capability to respond) (Crossler et al., 2017). In short, PMT research demonstrates that people must be both willing and able to respond to cyber security threats.

In order to understand willingness and ability, this research aims to better understand the factors that influence employees' security behaviour. With this knowledge, organisations can introduce technical preventive measures, policies, security training, regular communications of security risks, or enforce sanctions for non-compliance, amongst other strategies designed to improve cyber security safety. In addition to motivation, the psychological needs of end-users are also important in the design of information security systems. Further, people need to be positively disposed towards the object (i.e. cyber safety) in order to strive for it. Thus, the emotions employees feel towards information security requirements are significant in a safe cyber security system (Kraus et al., 2017). Additionally the knowledge and skills of users are important, which is why a premise of other research is that people with better security skills and risk awareness will be more likely to comply with security policies; and if they are fearful of sanctions, people will be less likely to violate security policies (Guo and Yuan, 2012; Vance and Siponen, 2012).

However, fulfilling ~~increasing~~ security controls and requirements requires additional effort, time, and skills, which can lead to employees' security compliance stress, especially when such activities are extended over time (Furnell and Thomson, 2009; Lee et al., 2016). Employees may find security controls inconvenient, tedious, and difficult to follow as well as impeding their work (Pham et al., 2016). Complying with security controls is an energy-draining process that leads to security fatigue in which it simply gets too hard or burdensome for users to maintain security (Furnell and Thomson, 2009). Regularly dealing with security controls such as system updates and notifications from firewalls, antivirus software and access controls, without much evidence of their effectiveness and necessity, can reduce security attention, and can therefore result in negative attitudes toward security tasks, ~~hence~~ lower~~ing~~ users' overall security performance (Day et al., 2017; Furnell and Thomson, 2009). Consequently, security requirements themselves can become a source of discouraging

employees' security compliance due to the demands (e.g. time, effort, frustration) on them (Pham et al., 2016, Posey et al., 2011a).

Information security stress has recently gained attention in behavioural security research. For example, Lee et al. (2016) examined security stress caused by work overload and privacy invasion from an individual's perspective, and how individual's security knowledge and their understanding of perceived threats can mitigate stress. D'Arcy et al. (2014) extended the techno-stress phenomenon to examine security-related stress caused by security overload, complexity and uncertainty. They found that such stress increases security violations. In a further study on the effects of stress on compliance, Pham et al. (2016) employed a qualitative approach in examining security burnout, which is a form of physical and psychological exhaustion over performing security-related tasks. The study also explored the organisational resources that support employees' security compliance. These studies have affirmed that stress from information security compliance exists and can negatively affect users' continued efforts in taking appropriate security measures. However, little research appears to have addressed how information security stress can be mitigated from both individual and organisational perspectives.

In this study, we aims to establish a theoretical basis for further studying the phenomenon of security burnout and its role in security management. We argue that security burnout may occur because of the combination of high and complex security demands where the individual lacks resources (organisational and personal) to cope with those demands. We aim to examine the impact of security demands on security burnout and examine to what extent organisational and personal resources can mitigate security stress based on the Job Demands-Resources (JD-R) model, a work stress theory (Demerouti et al., 2001).

The rest of this paper is organised as follows. First, we review security compliance burnout, sources of burnout, and factors that may mitigate burnout and stress. We then introduce the theoretical model and hypotheses and explain the research design, before presenting the results. Finally, we discuss the study's theoretical and practical implications, along with some suggestions for future research.

2. Literature review

Work-related stress is a major contributor to lower levels of productivity and compliance with organisational requirements. Measuring work-stress has often been undertaken via the JD-R model. It posits that employees' performance and well-being can be affected by both job demands and the resources available to support those demands. Individuals' performance and coping capacities are moderated via the competing motivational processes of work burnout and engagement (Demerouti et al., 2001). In later research, personal resources such as self-efficacy and experience have been

included in the extended JD-R model as a moderating factor between demands, resources, burnout and engagement that influence job performance, commitment and satisfaction (Bakker et al., 2010; Bandura, 1997; Toner et al., 2012). Both personal resources and organisational resources are used to comply with the demands of the job. If the job requirements demand more resources than there are available, negative stress and burnout can occur. Burnout describes a state of mental weariness, which includes two dimensions, exhaustion and cynicism, reflecting a distant attitude towards work (Schaufeli and Bakker, 2004). The concept of job demands and associated burnout can be extended to security demands and compliance burnout due to the fulfilment of security demands (Lee et al., 2016).

A key component of the JD-R model is job demands, which covers the physical, social, or organisational aspects of a job. Examples of job demands are work overload, complexity and job insecurity (Demerouti et al., 2001). The higher the job demands, the greater the effort, including the physical and psychological costs, that an employee must spend to achieve their goals, maintain performance and prevent psychological exhaustion (Day et al., 2017; Lavoie-Tremblay et al., 2010). As a result of high demands, unremitting fulfilment of job demands can incur prolonged physical and psychological costs, eventually leading to work burnout – a negative psychological state. Work burnout is a main determinant of undesirable employee behaviour, such as low work productivity and deviance (Gilboa et al., 2008), negative job strain and impaired health (Demerouti et al., 2009), as well as psychological distress (Bruck et al., 2002).

Complying with security requirements can require additional effort and time, which can lead to physical and psychological exhaustion over extended time periods (Demerouti et al., 2001). Few studies have examined how users develop cognitive and emotional stress due to continuing fulfillment of security demands. The impact of stressful security demands on security behaviour can be assessed under the phenomenon of technology-stress caused by human cognitive limitations and inability to adapt to rapid advances in technology (Shu et al., 2011). Information overload, as well as uncertainty and complexity of information systems can lead to technology stress in IT users, which may negatively influence technology use and productivity (Salanova et al., 2013). Under technology-stress, employees can feel negative affective experiences, such as exhaustion, scepticism and inefficacy towards the use of ICT, which then reduces professional commitment and undermines effective use of the technology.

There is a significant lack of information system literature that explores ~~what~~ aspects of security demands constitute negative or stressful compliance requirements that can affect security behaviour (D'Arcy et al., 2014). The nature of security tasks (i.e. complex, stressful and continuously changing) can cause burnout and increase moral and/or affective disengagement, which may lead to security non-compliance. In this study security compliance burnout refers to psychological exhaustion and cynicism toward complying with assigned security tasks and exercising security precautions. We

~~conceptualise~~ that burnout is due to the existence of high security demands and lack of resources, employees experience burnout as an energy-draining process that results in fatigue and cynical views about security programs. Such negative psychological affective experiences can reduce cognitive attention and focus, as well as commitment to performing security compliance tasks.

However, the JD-R model does not include relevant predictors of employees' work burnout (Crawford et al., 2010), nor does the model specify which resources are effective in safeguarding against burnout. Measuring security burnout in practice is still a challenge and lacks a solid theoretical framework to identify its sources. Earlier work has identified a number of contributing factors such as sustained effort, difficulty and perceived importance of security tasks (Furnell and Thomson, 2009). Similarly, no specific security resources have been identified that effectively reduce security demands associated with physical and psychological costs in achieving individual security requirements. This study endeavours to develop a model that details sources of security demands and resources (organisational and personal) contributing to security compliance burnout.

The following sections present analysis of key components of the JD-R model in the context of security compliance considering its organisational and individual personal characteristics.

2.1. Organisational security demands, resources and security compliance burnout

Security demands are tasks and procedures that employees must perform as part of their work responsibilities, such as accessing security policies for instructions and guidance, acquiring the skills and knowledge employees need to deal with changing security environments, and using security measures (Vacca, 2013). Coping with overloading security demands can increase compliance burnout, because security demands put time pressure on employees to complete other job duties (D'Arcy et al., 2014). People can view security tasks as inconvenient, work hindering and time-consuming, making them a legitimate reason ~~for not utilising~~ a security measure (Bulgurcu et al., 2010; Schneier, 2008). For example, an automated virus scan can disrupt an employee's intended work task because his or her computer slows down during the scan. Impeding work was reported to increase the perceived cost of compliance (Bulgurcu et al., 2010), and negatively impact compliance intentions (Dhillon and Torkzadeh, 2006; Vance and Siponen, 2012). One of the most common issues with security demands is that security compliance can negatively affect employees' work and consequently reduce their productivity (Pham et al., 2016). Security compliance *overload* refers to the amount of time and effort needed to perform security tasks in the working time available, which reduces an employee's productivity and increases their stress levels.

Security compliance burnout reflects both the psychological exhaustion and cynicism towards assigned security tasks and security precautions. Burnout can occur when people have been overloaded for extended periods of time. Performing a high and/or frequent number of security measures requires IT users to spend extra time and handle workflow disruption, while still being required to quickly respond to other work demands. This can create anxiety and tension, as well as make sustained mental attention difficult, thus reducing security efforts overall (Salanova et al., 2013). Hence, we hypothesise the following:

H1: Security compliance overload is positively related to security compliance burnout

Security policies provide formal guidelines and resources that specify user responsibilities when dealing with organisational information (von Solms and von Solms, 2004). Users need to access security policies for relevant information about their compliance needs. Boss et al. (2009) also acknowledge the importance of providing clear security specifications in order to achieve desired security compliance. Perceived quality and usefulness of security policies positively affected actual security compliance (Pahnila et al., 2007). However, employees commonly ~~identified~~ the need to access traditional written IT and security policies as a source of frustration and ~~disengaging~~ (Pham et al., 2016). That study also found that written policies were of little use in providing security practice guidance, and were considered as lengthy and difficult to read due to the use of unfamiliar terms. Accordingly, we hypothesise that:

H2: The need to access security policies is positively related to security compliance burnout

To fulfil security requirements, which can vary in complexity, users may need to acquire a certain level of computer and/or security knowledge and ~~to~~ spend time in applying security measures to their systems (Ashenden and Lawrence, 2013). Compliance burnout also occurs when security tasks require extra time, computer experience and/or security knowledge which employees may not possess (Pham et al., 2016), and this lack of skill can lead to stress (D'Arcy et al., 2014). In other words, an imbalance between a person's capabilities and security demands can also create stress or burnout, either when there is an anticipation of negative consequences due to inadequate responses (Chen et al., 2012-2013), or the requirements exceed one's capabilities and personal resources (Posey et al., 2011b). Thus, we hypothesise:

H3: High security skill requirements are positively related to security compliance burnout

Organisational resources are the physical, social or organisational aspects of the job that help facilitate achievement of work goals by reducing job demands' associated costs, and promoting personal growth and development (Demerouti et al., 2001). Depending on the nature of security demands, users may need different resources to comply properly. Perceptions about the organisation's security response efficacy are a factor in motivating employees to take protective measures against security

threats (Ifinedo, 2011; Vance et al., 2012). The resources and security measures that an organisation provides to facilitate employees' security compliance can reduce the demands on the individual's IT efforts and ~~also~~ demonstrate the effectiveness of organisational security measures. Furthermore, users are more likely to perform security activities when they understand the purposes of the security program, perceive security measures to be relevant and effective against risks, and when they believe they are capable of fulfilling such tasks (Vance and Siponen, 2012~~;~~ Vance et al., 2012). Thus, users are more likely to use their personal resources to comply when they perceive that the organisation is upholding their part of a cyber-security system.

Some organisational resources that could help employees in reducing burnout and improving compliance include security response efficacy, individual compliance evaluation, and security compliance autonomy (Pham et al., 2016). Security response efficacy ~~comprises~~ the effectiveness of organisations or IT departments in communicating and supporting end-users ~~in understanding~~ how to comply with security requirements. Response efficacy can be measured in terms of timely and helpful IT support~~;~~ IT staff competences and perceived IT value in the organisation (Pham et al., 2016). Response efficacies are required to reduce the impact of IT security systems on employees' work by ensuring compliance time and effort are minimal. For example, a responsive and effective help desk can reduce work interruption, offset the effects of decreased productivity, and increase employees' satisfaction (Salanova et al., 2013). Security compliance autonomy represents the independent ability of users to use their personal skills in maintaining security compliance.

Formal evaluation including rewards and sanctions of individual IT effective security compliance has been identified as an effective way to motivate on-going compliance. For example, financial rewards were found to have an impact on security compliance (Boss et al., 2009; Bulgurcu et al., 2010; Siponen et al., 2014). In addition, compliance evaluation should also include penalties for non-compliance, such as losing a bonus, pay cut or even disciplinary actions. Participants in Pham et al.'s (2016) study explained that formal evaluation of security compliance demonstrated ~~the~~ organisations took IT security seriously and therefore the individual would work harder to maintain their part of the cyber security system. In that study, employees only ~~make~~ information security compliance a personal responsibility when the organisation ~~recognise~~ IT security efforts at different levels of achievement, including non-performance. However, it is not known how these rewards and sanctions affect security overload or burnout.

Security compliance autonomy is where individuals have an ability to act on IT security issues, using their personal skills and competences, in the fulfilment of their roles. In their 2016 study, Pham et al. interviewed IT users about IT security. Users favoured security programs that balanced work and personal requirements and systems that provided flexibility to respond to demands. Users were not pleased with security controls that took away their autonomy in deciding which software settings and

applications to use for work. Strict control of security settings was perceived to hinder job performance and reduce productivity. In the absence of compliance autonomy, users would comply passively and simply delegate security responsibility to the IT department, thereby absolving themselves from undertaking security tasks at all. The study showed that end-users are seeking to be active participants in developing skills that enable and empower them, not passive receivers of procedural information (Pham et al., 2017).

The organisational resources namely organisational security response efficacy, rewards, sanctions and security skill use and development discussed above are theorised to reduce users' perceived burnout as they minimise time-consuming tasks, reduce complexity and increase intrinsic motivation to complete security tasks. In this study, the '*organisational resources for security*' construct was assessed as a second-order construct within the JD-R model (Bakker and Demerouti, 2007). Therefore, we put forward the following hypothesis:

H4: Organisational security resources are negatively related to security compliance burnout

The following section presents a review of how one might use personal resources to deal with security compliance burnout.

2.2. Personal resources and security compliance burnout

Another resource available to ~~the~~ employee in fulfilling job demands is personal resources. The original JD-R model mainly addresses the influence of work-related factors – demands and resources = on people's stress and job commitment, without incorporating their personal resources (Schaufeli and Taris, 2014; Xanthopoulou et al., 2007). Personal resources are mental and emotional self-competences that can affect how an individual appraises the work environment, copes with stress, and recovers from ~~the~~ stressful periods (Hobfoll et al., 2003). Thus, when applied to security behaviour, personal resources could be effective in coping with security demands and alleviating the negative impact of compliance burnout on compliance behaviour.

One personal resource is self-efficacy, which relates to an individual's belief in their ability to successfully perform their security tasks, as well as to cope with changing requirements. Self-efficacy theories are derived from social cognitive theory (SCT) and have been researched in the IT security context (Posey et al., 2015). According to SCT (Bandura, 1997) and theory of planned behaviour (Ajzen, 1991), self-efficacy influences one's ability to mobilise motivation, deploy cognitive resources, and engage with emotional reactions, such as stress and anxiety, in response to a task. IT self-efficacy has been shown to affect anxiety related to ~~Information and Computer Technology (~~ICT~~)~~ (Henderson et al., 1995), motivate continued computer use (Deng et al., 2004), and to help safeguard against burnout (Salanova et al., 2000). Further, Xanthopoulou et al. (2007) found that highly self-

efficacious employees adapt better to a changing and challenging work environment, focus more on work resources than work demands, and experience higher levels of engagement. Additionally, employees' resources can moderate the tension between work demands, work resources, and perceived burnout that influences individual job performance, commitment and satisfaction (Bakker et al., 2010; Toner et al., 2012).

According to Shu et al. (2011), employees with high security self-efficacy are willing to overcome the complexities of the security tasks and cope with them more positively, decreasing the level of perceived compliance burnout by the employees . Hence, the following hypothesis is put forward:

H5: Security self-efficacy is negatively related to security compliance burnout

Exposure to security incidents, such as a virus infection, losing information, and online fraud causes a negative emotional state such as fear, stress or anxiety, which could lower individuals' belief in their security self-efficacy (Rhee et al., 2009). It is feasible that higher levels of exposure increase users' perceptions of threat (Rhee et al., 2009) and lack of ability to deal with security tasks would increase a sense of burnout. Rhee et al. (2009) found that prior security failure incidents reduce perceived security self-competences, which consequently reduces users' intention to strengthen security efforts. Further to this effect, experiencing a serious security incident (increased exposure) may increase the perceived cost of non-compliance (Bulgurcu et al., 2010) and create a negative emotional state, such as anxiety or stress and increasing the risk of burnout. Therefore, the following hypothesis is proposed.

H6: Security exposure is positively related to security compliance burnout

Figure 1 depicts the theoretical model of this study.

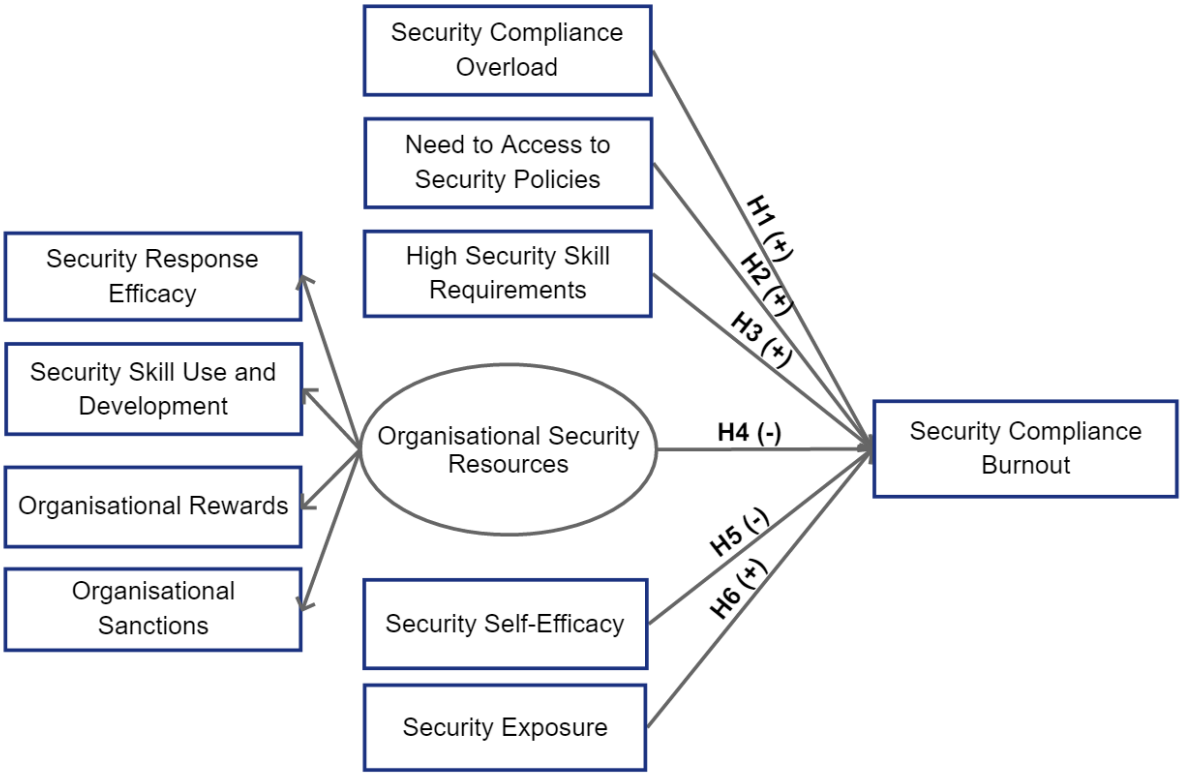

Figure 1: Theoretical model of Security Compliance Burnout

3. Research design

3.1. Measurements

The research constructs employed in this study were measured with previously used measures and items provided they satisfied three conditions: (1) they have measured the same concepts as the study, (2) they were empirically tested and validated, and (3) they were designed for a similar group of participants (Schrauf and Navarro, 2005). The present study examined existing literature in the domain of security management, security policies, and security compliance to find relevant scales. Some ~~of~~ survey items were adapted and developed for this study. Table 1 shows constructs, operational definitions, theoretical sources, and measurement item sources. All variables were measured using a seven-point Likert-type scale.

Table 1: Specification of the construct domain and measurement items

Domain	Construct	Definition/Description	Construct Sources	Measurement items source	Items
Organisational Security Demands	Security compliance overload	Having too many security tasks to do in the time available	Bulgurcu et al. (2010); Herath and Rao (2009b); Vance et al. (2012)	Bulgurcu et al. (2010)	3
	Difficult access to security requirements	Time-consuming access and unclear guidance from documented security policies and procedures.	Adapted from Boss et al. (2009)	Adapted from Boss et al. (2009)	4
	Security skill requirements	The pressure to spend time and effort in learning and understanding IT in order to comply with the organisation's security requirements.	Shih et al. (2011)	Adapted from Shih et al. (2011)	3
Organisational Security Resources	Security response efficacy	Level of satisfaction with the clarity and usefulness of the organisational security resources.	Pahnila et al. (2007)	Adapted from Pahnila et al. (2007)	4
	Security skill use and development	Opportunities to use and develop one's skills in performing security tasks as required by the organisation.	Workman et al. (2008); Wall et al. (1996)	Adapted from Wall et al. (1996)	4
	Organisational rewards	Tangible or intangible compensation that an organisation gives to an employee in return for compliance with security requirements.	Boss and Kirsch (2007); Bulgurcu et al. (2010)	Boss and Kirsch (2007)	4
	Organisational sanctions	Disciplinary actions towards non-compliance. Sanctions can be described in terms of financial/non-financial	Boss and Kirsch (2007)	Boss and Kirsch (2007)	3

		penalties.			
Personal Resources	Security self-efficacy	An employee's judgment of personal skills, knowledge, or competency about fulfilling the requirements of the security demands.	Bulgurcu et al. (2010); Vance et al. (2012); Workman et al. (2008); Rhee et al. (2009)	Adapted from Rhee et al. (2009)	6
	Security exposure	The extent to which users have had direct knowledge or experience of security incidents in their own lives (e.g. security issues happening to them or to friends/family, as well as things that they may have internalised from media coverage).	Rhee et al. (2009)	Adapted from Rhee et al. (2009)	4
	Security compliance burnout	Psychological exhaustion and cynicism towards assigned security tasks. It shows a lack of interest and underestimation of security issues and measures.		Adapted from Schaufeli et al. (1996); Boss et al. (2009)	5
				Total items	40

3.2. Data collection and sample characteristics

The sample of this study were employees working in organisations in Vietnam who used networked computer applications such as email or accessed networked internet as part of their job on a daily basis. It was expected that the relatively large-scale organisations that were selected to participate in the survey would have some form of information security policies or security guidance to explain proper use of information technology. Further, consistent with other studies, it was expected that organisation size would provide an indication of the level of security demands and resources. An organisation with a larger number of users will normally have more security demands and provide more appropriate security resources. Participants for the survey were recruited through the authors' networks: friends, family members, colleagues, University alumni, and the researchers' personal

Facebook pages. To ensure the representativeness of the sample, participants were recruited in various industries in three biggest cities in Vietnam ~~including~~ Ho Chi Minh City, Hanoi, and Da Nang.

Vietnam has a high mobile cellular penetration rate at 147 subscriptions per 100 people, and 48.3% of the population accessed the internet in 2017 (Source: United Nations Conference on Trade and Development, Foreign Direct Investment Online database). In a 2015 survey by Antivirus and Internet Security Solutions (ESET), Vietnam ~~has been~~ ranked lowest in cyber security awareness amongst Malaysia, Singapore, India, Thailand, Hong Kong, and Indonesia (ESET, 2015). Over the first three months of 2018, Vietnam was ranked 11th in the list of the 20 countries in the world facing the highest risk of local infection from removable media connected to computers (USB flash drives, camera and phone memory card, and external hard drives); number three for being attacked by Trojan cryptos; and placed in top 20 countries where users faced the risk of online infection (Chebyshev et al., 2018). Given the fast growing economy of Vietnam and its commercial connections across the globe, it is important to understand the Vietnamese context in order to decrease cyber risks globally.

4. Data analysis and results

Testing of the proposed theoretical model followed a two-step structural equation model (SEM) building approach (Anderson and Gerbing, 1988; Hair et al., 2010). The first step involved assessing the validity of the proposed measurement model. If the measurement model ~~is~~ satisfactorily obtained, the second step ~~is~~ to assess the validity of the structural model. Data were analysed using SPSS V.20 and AMOS V.20.

4.1. Demographic ~~I~~information

The sample consisted of 443 participants. Most of the participants were between 18 and 34 years old ~~(74.7%),~~ an age group that is representative of the relatively young labour force in Vietnam. More than 82% of participants had undergraduate (63.1%) and postgraduate degrees (17.9%), 12.7 per cent had a diploma, and 6.4% had completed high school. The figures show a relatively high education level of the workers in the participating companies. The majority of the participants held non-managerial positions (71.3%). The top three industries of participants and companies were finance and insurance, trading and commerce, and IT-software development at 31.6%, 20.5% and 13.4%, respectively. Other industries represented were education (8.7%), transport (8.1%), building and manufacturing (6.5%), medical services (3.4%), and others (6.5%). 3.8 per cent of the participants did not indicate their industry. Most of the participants (59.2%) worked in companies with ~~workforce~~ between 11 and 200 employees. Additionally, 14.6% of participants worked in companies with 200-500 employees, 16% in large companies with more than 500 employees and 9.9% in companies with less than 10 employees.

As the availability of IT usage policies and the frequency of access to such policies are important to security compliance, participants were asked to disclose when they last accessed their organisation's IT policy. This information provided some background on the availability of (organisational resource) and users' engagement with corporate policies about IT security (personal resource). Table 2 shows that 64.2% of the participants accessed an IT policy ~~access~~ within the last 12 months, whilst 18.4% had never read an IT security policy, and 17.4% disclosed that there was no IT security policy in their current company. A general lack of security knowledge may be explained by these results, indeed the significant proportion of 'never accessed' and 'no IT policy' is an area of concern for those seeking to embed IT security in their organisation. While it is feasible that the IT policies do exist and participants have been ill-informed, it still indicates a lack of communication about IT security overall.

Table 2: Frequencies of access to IT Policies

Characteristic	Value	Frequency	%	Cumulative %
Access to IT Policies	Last month	106	25.3	25.3
	Last 6 months	99	23.6	48.9
	Last 12 months	64	15.3	64.2
	Never	77	18.4	82.6
	No IT security policy	73	17.4	100.0
	Missing	24	5.4	

Tables 3 and 4 provide data on IT policy access and the level of IT use analysed by company size. As shown in Table 3, participants from companies with 500 to 1000 staff reported the highest level of policy access in the last six months (65.2%), followed by those from companies with more than 1000 staff (64%), 11-200 (46.4%), 1-10 (45.3%), and 201-500 (43.1%) respectively.

Table 3: Access IT policies by Company Sizes

Company size	Last month	Last 6 months	Last 12 months	Never accessed	No IT security policy
1-10	12 (28.6)	7 (16.7%)	4 (9.5%)	11 (26.2%)	8 (19%)
11-200	50 (21.5%)	58 (24.9%)	42 (18%)	40 (17.2%)	43 (18.5%)
201-500	11 (19%)	14 (24.1%)	10 (17.2%)	15 (25.9%)	8 (13.8%)
501-1000	7 (30.4%)	8 (34.8%)	2 (8.7%)	1 (4.3%)	5 (21.7%)
Above 1000	11 (44%)	5 (20%)	3 (12%)	5 (20%)	1 (4%)
Total	91 (23.9%)	92 (24.1%)	61 (16%)	72 (18.9%)	65 (17.1%)

Table 4 indicates that the larger the company, the higher use of IT facilities. For example, 91.3% of participants from large firms (over 1000 employees) reported a high use of IT, while 66.7% of mid-size companies (501-1000), 63.8% from both 11-200 and 201-500 sized companies, and only 46.3% of very small companies (less than 10 employees) indicated high level of IT usage. Hence, it is reasonable to assume that larger companies would provide higher level of IT resources and requirements to their users.

Table 4: Level of IT use by Company size

Company size	High level use of IT
1-10	19 (46.3%)
11-200	148 (63.8%)
201-500	37 (63.8%)
501-1000	16 (66.7%)
Above 1000	21 (91.3%)

4.2. Measurement model

In order to assess the validity of the measurement model, the validity of individual measures were assessed by analysing the convergent and divergent validity of the constructs and the overall fit. All ten constructs were defined as reflective constructs as the measured items ~~are~~ interchangeable in the questionnaire, and each ~~have~~ a common theme (Petter et al., 2007).

First, reliability of all constructs was tested to ensure the measures of the same construct ~~are~~ related to each other, before testing the construct validity. Reliability can be measured using two statistical indicators: item-total correlation, which should exceed 0.5 and Cronbach's alpha (>0.7) (Hair et al., 2010) (see Table 5). Item ASP2 ("*I'm required to know a lot of existing written policies and guidelines to ~~security~~ my computer system*") ~~has~~ a lower item-total correlation than the 0.5 threshold. This means that a formal requirement to access policies may not be practical to users in the context of Vietnamese organisations. Item ASP2 was removed and the final research instrument contained 39 variables, from ten constructs.

Convergent validity examines whether measured items of the same construct are correlated, which can be assessed through factor loading, average variance extracted (AVE), and reliability (Hair et al., 2010). Table 5 summarises the results of the convergent validity testing of all constructs. Composite reliability (CR) values of all constructs were above the 0.7 threshold (Nunnally and Bernstein, 1994). AVE values of all constructs were greater than 0.5 (Hair et al., 2010). Hence, all first-order constructs had acceptable reliability and convergent validity.

Table 5: Results of reliability and convergent validity of first-order constructs

Construct	Item	Item-Total Correlation (>0.5)	Status	Cronbach's Alpha (>0.7)	AVE (>0.5)
Security compliance overload (SCO)	SCO1	0.763		0.889	0.737
	SCO2	0.846			
	SCO3	0.741			
Difficult access to security requirements (ASR)	ASR1	0.594		0.786	0.567
	ASR2	0.472	Removed		
	ASR3	0.676			
	ASR4	0.638			
High security skill requirements (SSR)	SSR1	0.689		0.824	0.612
	SSR2	0.682			
	SSR3	0.674			
Security response efficacy (SRE)	SRE1	0.615		0.786	0.507
	SRE2	0.646			
	SRE3	0.588			
	SRE4	0.525			
Security skill use and development (SSUD)	SSUD1	0.623		0.848	0.638
	SSUD2	0.773			
	SSUD3	0.739			
	SSUD4	0.619			
Organisational rewards (ORW)	ORW1	0.672		0.864	0.597
	ORW2	0.758			
	ORW3	0.733			
	ORW4	0.692			
Organisational sanctions (OS)	OS1	0.735		0.87	0.664
	OS2	0.71			
	OS3	0.761			
Security self-efficacy (SSE)	SSE1	0.756		0.92	0.650
	SSE2	0.799			
	SSE3	0.8			
	SSE4	0.771			
	SSE5	0.739			
	SSE6	0.772			
Security exposure (SE)	SE1	0.584		0.779	0.522
	SE2	0.514			

	SE3	0.609			
	SE4	0.632			
Security compliance burnout (SCB)	SCB1	0.702		0.899	0.649
	SCB2	0.769			
	SCB3	0.794			
	SCB4	0.757			
	SCB5	0.723			

The construct of organisational security resources was assessed as a second-order construct, similar to testing first-order constructs: CR and AVE for the second-order construct of organisational security resources (OSR) were calculated, and satisfied recommended convergent validity thresholds (see Table 6).

Table 6: Results of convergent validity testing for second-order construct of organisational security resources

Second-order construct	First-order construct	CR (>0.7)	AVE (>0.5)	Convergent Validity
OSR	SRE	0.793	0.492	Satisfactory
	SSUD			
	OS			
	ORW			

Discriminant validity looks for differences of correlation among distinct but similar factors. High discriminant validity verifies that a construct is unique and the measured items capture a factor that other measures do not. Discriminant validity for all constructs was satisfied, as the squared root of AVE estimates for two constructs was greater than the correlation coefficients between the constructs (see Table 7) (Hair et al., 2010).

Table 7: Squared root of AVE and correlation between constructs

	SCB	ASR	SSR	SCO	SSE	SE	OSR
Security compliance burnout (SCB)	**0.806**						
Difficult access security requirements (ASR)	0.347	**0.753**					
High security skill requirements (SSR)	-0.028	0.393	**0.782**				
Security compliance overload (SCO)	0.407	0.388	0.116	**0.858**			
Security self-efficacy (SSE)	-0.020	-0.015	0.100	-0.064	**0.806**		

Security exposure (SE)	0.146	0.242	0.317	0.076	0.434	**0.723**	
Organisational security resources (OSR)	0.016	0.166	0.382	0.154	0.611	0.278	**0.703**

* *The bolded diagonal elements are the squared root of the AVE scores*

The resultant measurement model was tested again for model fit. Goodness of fit (GOF) in the measurement model indicates the ability of a model to reproduce the data (i.e., the similarity of the observed and estimated covariance matrices among measured items). GOF tries to find which model reflecting the underlying theory best represents the data. Model fit is one of the most important steps in structural equation modelling (Yuan, 2005). The fit statistics are shown in Table 8.

Table 8: Fit statistics of the measurement model

Model Fit Statistics	
CMIN = 1281.67 Df = 600 CMIN/df = 2.13 p-value = .00	CFI = .919 RMSEA = .05, 90% CI for RMSEA = (0.049, 0.057) PCLOSE = .115

The statistics indicate an adequate model fit. The CMIN/DF at 2.13 is almost at the upper bound 2 cut-off value. The RMSEA at 0.05 is less than the upper limit of 0.07 and the PCLOSE at 0.115 is much greater than the upper 0.05 threshold .07 (Steiger, 2007). The 90 per cent confidence interval for this RMSEA shows that even with the upper bound, RMSEA at 0.057 is still adequate. The CFI at 0.919 is above the 0.90 rule of thumb cut-off fit value (Hu and Bentler, 1999).

4.3. Structural model

The testing results of the structural model indicated an adequate fit. The CMIN/DF of the model at 2.33 was slightly above the upper-bound 2 cut-off value, the RMSEA at 0.05 is less than the upper limit of 0.07. Finally, the CFI at 0.90 is lower than the 0.92 threshold for a model of over 30 variables (Hair et al., 2010), though it satisfies the 0.90 rule of thumb cut-off fit value (Hu and Bentler, 1999). See Figure 2 for a visualisation of results.

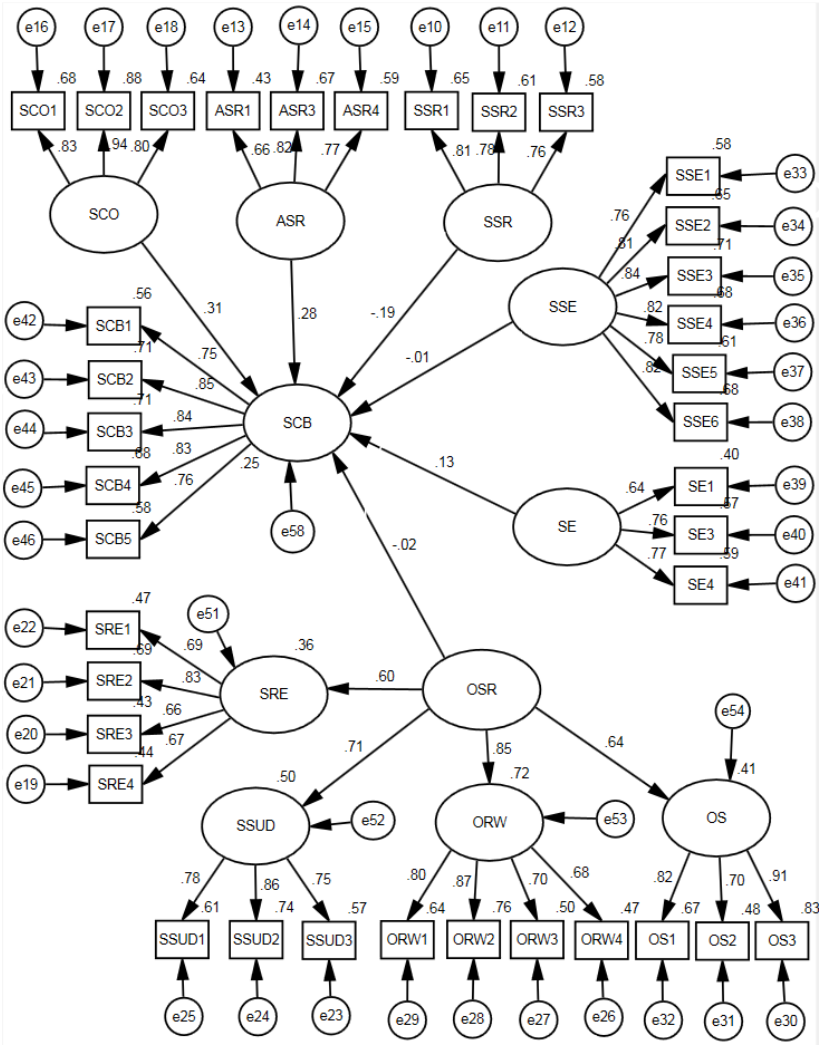

Figure 2. Structural model assessment results

Table 9 summarises the results of the hypothesis testing. Both hypotheses H1 (effect=0.31, p<0.001) and H2 (0.28, p<0.001) were supported, though H3 (effect=-0.19, p<0.001) was found to reduce security compliance burnout instead, hence H3 ~~is~~ not supported. Hypotheses H4 (effect=-0.02, p>0.05) and H5 (effect=-0.01, p>0.05) ~~are~~ not supported due to non-significant relationships at the 95 per cent confidence interval. Finally, H6 ~~is~~ supported (effect=0.13, p<0.05).

Table 9: Hypotheses testing results

Hypothesis	Standardised Path Estimate (Effect)	Hypothesised Direction	P-value (<0.05)	Supported?
H1: Security compliance overload is positively related to security compliance burnout.	0.31	Positive	0.001	Yes
H2: Difficult access to security requirements is positively related to security compliance burnout.	0.28	Positive	0.001	Yes
H3: High security skill requirements are positively related to security compliance burnout.	-0.19	Positive	0.01	No
H4: Organisational security resources are negatively related to security compliance burnout.	-0.02	Negative	0.40	No
H5: Security self-efficacy is negatively related to security compliance burnout.	-0.01	Negative	0.94	No
H6: Security exposure is positively related to security compliance burnout	0.13	Positive	0.01	Yes

5. Discussion

This study showed that the three categories of security demands had different impacts on compliance burnout, while organisational resources and security self-efficacy were not significantly related to burnout, security exposure was positively related to it (Table 9). Overall, the theoretical model developed in this research explained 25% of the variance in IT users' burnout (Figure 2), which is considered a weak but adequate level for practical implication (Cohen, 1998). Each of the antecedents to security compliance burnout are discussed in the following sections.

5.1. Mixed impacts of security demands on compliance burnout

The structural analysis shows security compliance overload and poor access to security requirements were positively related to compliance burnout, whereas high security skill requirements were negatively related to it. Security compliance overload was positively related to and had the strongest impact on security compliance burnout (effect=0.31, $p<0.001$) of the three components of security demands. The positive relationship between security compliance overload and burnout further emphasises the issue of security task overload, where professionals have to work harder and faster while simultaneously dealing with multiple applications and tasks (D'Arcy et al., 2014; Lee et al., 2016). This is consistent with Salanova et al. (2013), who found that completing security measures can add to workloads of already stressed staff. IT users in such circumstances struggle to cope with workflow disruptions, as well as dealing with security measures. Users can become anxious and tense and these negative emotions make sustained concentration difficult.

The results show that experience of security compliance overload varies depending on several factors.

Organisations may not clearly require IT users to perform security tasks, especially when they place more reliance on technical measures than users' compliance. These organisations may automate most security measures and minimise the impact of security compliance on employees' work. For example, Pham et al. (2016) found that some participants did not perceive the workload associated with security compliance as significant and did not feel that it negatively affected their work. Organisations may not implement security measures to protect their information assets, thus users do not experience the their impact on their work (Pham et al., 2016). Users may ignore or delay security tasks. As IT users may not exert time and effort to protect the information assets of the organisation, they may not experience much compliance overload (Herath and Rao, 2009b).

The results in Table 9 indicate that difficult and time-consuming access to written security policies increases burnout (effect=0.28, $p<0.001$). This finding emphasises that traditional methods of disseminating policies and procedures may need to be reviewed. Security requirements and practice should be communicated just-in-time, using non-technical terms, possibly with graphic posters to decrease stress of access. Complex security documents 'hidden' on secure servers should not be the main source of cyber security instructions to IT users.

Contrary to the original expectation, high skill requirements significantly and negatively related to security burnout instead (effect=0.-19, $p<0.01$). This finding indicates that users may perceive skill-demanding security tasks as personally challenging and less tedious (i.e. self-motivating), which may encourage them to obtain skills to be more competent and engage in security activities. Moreover, Pham et al. (2016) also reported that users may find certain security measures unnecessary or excessive and become distant towards overall security initiatives regardless of their security skills. Consequently, these users can experience compliance burnout when called upon to perform required security tasks, even if they are self-efficacious.

5.2. Organisational security resources and compliance burnout

The results in Table 9 did not indicate a significant relationship between organisational security resources and security compliance burnout (effect=-0.02, p>0.05). Counter to expectations, the provision of organisational resources does not reduce IT users' compliance burnout.

This counter-intuitive result may be because some security tasks incur personal costs regardless of whether or not the organisation also provides supporting resources. For example, IT tasks incur response costs, such as additional time, work disruption, or complexity, irrespective of whether there are available organisational resources. As these are sunk costs, unable to be changed, this may result in users' burnout notwithstanding the existence of organisational security resources. Additionally, an organisation that provides adequate and effective security resources such as technical support, training, or rewards for compliance is often one that imposes more security measures and conducts more regular security check-ups. The introduction of such extensive measures can affect productivity and lead to even higher risk of burnout (Pham et al., 2016).

Compliance burnout might occur regardless of availability of resources but with different triggers for exhaustion and/or cynicism. For example, too many resources (or an inability to engage with resources) might contribute to exhaustion, and too little perceived support might contribute to a sense of cynicism.

Effective security resources to assist users' compliance, however, can result in users' over-reliance on the organisation for protecting information assets. For example, facilitating conditions such as the time to learn new skills, easy access to security policies and support to comply negatively influences attitudes towards compliance (Pahnila et al., 2007), contrary to the authors' original hypothesis. An explanation for this could be that users believe security responsibilities should be dealt with by the organisation through technical measures (Cox, 2012). Albrechtsen and Hovden (2009) explained that employees often left complex security tasks to organisations, and underestimated their own roles in security protection. This implies that the more effective organisational security resources, the more employees are prone to the traditional view that security is organisation's responsibility, therefore they will be less reliant on their own actions.

Finally, some components of security resources, especially rewards, may not actually be available at the surveyed organisations. Therefore, their impact on burnout was negative ~~merely~~ because they did not exist within the organisation. While several studies have mentioned that organisations rarely introduced financial rewards for security compliance (Guo and Yuan, 2012; Hu et al., 2011), the

concept of rewards and sanctions remains a key area of consideration for compliance motivation studies. This is a limitation that needs to be addressed in future research.

5.3. Personal security resources and compliance burnout

The results show that security self-efficacy does not have a significant relationship with compliance burnout. This may be due to a work environment where users may not have a substantial number of opportunities to use their security skills or requisite security tasks could be simple enough that they do not require much security self-efficacy. Furthermore, some security tasks can increase frustration from users regardless of their skills. For example, virus scanning may slow down the computer system and affect work productivity, and users cannot do much to speed up the process. In such cases, an employee can experience fatigue regardless of their self-efficacy due to time pressures and system-imposed constraints (Moody and Galletta, 2015). In such circumstances, secondary tasks such as virus scanning may be ignored to accomplish the primary work tasks.

6. Implications and future direction

This paper is one of the first studies to examine the sources and mitigating factors of security burnout, from both personal and organisational perspectives. The study demonstrates that security burnout is real and presents a danger to organisations seeking to maintain secure IT environments. There is certainly a ways to go but the role of human factors, as both as a barrier and a facilitator to secure cyber environments, cannot be ignored.

The introduction of security measures and polices aimed to protect and guide employees' cyber activities puts more workload and more stress on users. This sustained stress can reduce users' attention and efforts to continue their compliance. Using the JD-R model, a work-stress theory, this research showed that burnout may be a result of security-related overload and cumbersome access to security policies and instructions. The nature of security when it comes to security compliance is potentially a major issue; the more simple and tedious tasks, the more likely ~~the~~ user experiences security burnout, regardless of their self-efficacy. Organisational efforts to relieve users of responsibility by making things simple may therefore actually have deleterious effects on security.

This study also showed that easing security burnout can be a challenging task. Both organisational and personal resources combined barely reduce security burnout. Users not only need to feel that they can respond to cyber security risks (response efficacy), but also need to find such tasks challenging, not tedious and repetitive (autonomy-increasing and self-motivating). Consequently, burnout can occur regardless of training and development in security or access to organisational resources designed to effect cyber secure environments. To prevent burnout, organisations seeking to build

better infrastructure around cyber security need to decrease the complexity of the task, but not at the sake of autonomy and competency, which are major motivators for human performance.

Future research could identify effective measures in mitigating security burnout in practice, and how burnout-free compliance can influence security practice. However, as these results show, a burnout-free cyber security environment could be one where the user is completely ignorant of security initiatives and requirements.

References

Ajzen, I. 1991. Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes,* 50**,** 179–211.

Albrechtsen, E. & Hovden, J. 2009. The Information Security Digital Divide between Information Security Managers and Users. *Computers & Security,* 28**,** 476–490.

Anderson, J. C. & Gerbing, D. W. 1988. Structural Equation Modeling in Practice: A Review and Recommended Two-Step Approach. *Psychological Bulletin,* 103**,** 411-423.

Ashenden, D. & Lawrence, D. 2013. Can We Sell Security Like Soap? A New Approach to Behaviour Change *The New Security Paradigms Workshop (NSPW).* Banff, AB, Canada: ACM.

Bakken, B., & Torp, S. 2012. Work Engagement and Health among Industrial Workers. *Scandinavian Journal of Organizational Psychology*, 4(1), 4-20.

Bakker, A. B., Boyd, C. M., Dollard, M., Gillespie, N., Winefield, A. H. & Stough, C. 2010. The Role of Personality in the Job Demands-Resources Model: A Study of Australian Academic Staff. *Career Development International,* 15**,** 622-636.

Bakker, A. B. & Demerouti, E. 2007. The Job Demands-Resources Model: State of the Art. *Journal of Managerial Psychology,* 22**,** 309-328.

Bandura, A. 1997. *Self-Efficacy: The Exercise of Control*, New York: Freeman.

Boss, S. R., & Kirsch, L. J. 2007. The Last Line of Defense: Motivating Employees to Follow Corporate Security Guideliness. *Paper presented at the The 28th International Conference on Information Systems, Montreal*.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A. & Boss, R. W. 2009. If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. *European Journal of Information Systems,* 18**,** 151-164.

Bruck, C. S., Allen, T. D. & Spector, P. E. 2002. The Relation between Work-Family Conflict and Job Satisfaction: A Finer-Grained Analysis. *Journal of Vocational Behavior,* 60**,** 336-353.

Bulgurcu, B., Cavusoglu, H. & Benbasat, I. 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. *MIS Quarterly,* 34**,** 523-548.

Chebyshev, V., Sinitsyn, F., Parinov, D., Liskin, A. & Kupreev, O. 2018. *It Threat Evolution Q1 2018. Statistics* (Online). https://securelist.com/it-threat-evolution-q1-2018-statistics/85541/: SecureList. (Accessed 16 March 2018).

Chen, Y., Ramamurthy, K. & Wen, K.-W. Winter 2012-2013. Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems,* 29**,** 157–188.

Cohen, J. 1998. *Statistical Power Analysis for the Behavioral Sciences,* Hillsdale, NJ: Lawrence Erlbaum Associates.

Cox, J. 2012. Information Systems User Security: A Structured Model of the Knowing–Doing Gap. *Computers in Human Behavior,* 28**,** 1849-1858.

Crawford, E. R., Lepine, J. A. & Rich, B. L. 2010. Linking Job Demands and Resources to Employee Engagement and Burnout: A Theoretical Extension and Meta-Analytic Test. *Journal of Applied Psychology,* 95**,** 834-848.

Crossler, R. E., Bélanger, F. & Ormond, D. 2017. The Quest for Complete Security: An Empirical Analysis of Users' Multi-Layered Protection from Security Threats. *Information Systems Frontiers*, 1-15.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hud, Q., Warkentin, M. & Baskerville, R. 2013. Future Directions for Behavioral Information Security Research. *Computer & Security,* 32, 90-101.

D'arcy, J., Herath, T. & Shoss, M. K. 2014. Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective. *Journal of Management Information Systems,* 31, 285-318.

Day, A., Crown, S. N. & Ivany, M. 2017. Organisational Change and Employee Burnout: The Moderating Effects of Support and Job Control. *Safety Science*, 100 (Part A), 4-12.

Demerouti, E., Bakker, A. B., Nachreiner, F. & Schaufeli, W. B. 2001. The Job Demands-Resources Model of Burnout. *Journal of Applied Psychology,* 86, 499-512.

Demerouti, E., Le Blanc, P. M., Bakker, A. B., Schaufeli, W. B. & Hox, J. 2009. Present but Sick: A Three-Wave Study on Job Demands, Presenteeism and Burnout. *Career Development International,* 14, 50-68.

Deng, X., Doll, W. & Truong, D. 2004. Computer Self-Efficacy in an Ongoing Use Context. *Behaviour & Information Technology,* 23, 395-412.

Dhillon, G. & Torkzadeh, G. 2006. Value-Focused Assessment of Information System Security in Organizations. *Information Systems,* 16, 293-314.

Eset. 2015. *Việt Nam Đứng Cuối Khu Vực Về Nhận Thức an Ninh Mạng* (Online). ICTNEWS.VN. Available: http://ictnews.vn/cntt/bao-mat/viet-nam-dung-cuoi-khu-vuc-ve-nhan-thuc-an-ninh-mang-133308.ict (Accessed 23/03/2016 2016).

Furnell, S. & Thomson, K. L. 2009. Recognising and Addressing 'Security Fatigue'. *Computer Fraud & Security,* 11, 7-11.

Gilboa, S., Shirom, A., Fried, Y. & Cooper, G. A. 2008. Meta-Analysis of Work Demand Stressors and Job Performance: Examining Main and Moderating Effects. *Personnel Psychology,* 61, 227–271.

Guo, K. H. & Yuan, Y. 2012. The Effects of Multilevel Sanctions on Information Security Violations: A Mediating Model. *Information & Management,* 49, 320-326.

Hair, J. F., Black, W. C., Babin, B. J. & Anderson, R. E. 2010. *Multivariate Data Analysis*, Pearson Education Inc.

Henderson, R. D., Deane, F. P. & Ward, M. J. 1995. Occupational Differences in Computer-Related Anxiety: Implications for the Implementation of Acomputerized Patient Management Information System. *Behaviour & Information Technology,* 14, 23–31.

Herath, T. & Rao, H. R. 2009a. Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems,* 47, 154-165.

Herath, T. & Rao, H. R. 2009b. Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of Information Systems,* 18, 106-125.

Hobfoll, S. E., Johnson, R. J., Ennis, N. & Jackson, A. P. 2003. Resource Loss, Resource Gain, and Emotional Outcomes among Inner City Women. *Journal of Personality and Social Psychology,* 84, 632-643.

Hu, L. T. & Bentler, P. M. 1999. Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Critera Versus New Alternatives. *Structural Equation Modeling,* 6, 1-55.

Hu, Q., Xu, Z. C., Dinev, T. & Ling, H. 2011. Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Communications of the ACM,* 54, 54-60.

Ifinedo, P. 2011. Understanding Information Systems Security Policy Compliance: An Integration of the Theory of Planned Behavior and the Protection Motivation Theory. *Computers & Security,* 31, 83-95.

Johnston, A. C., Warkentin, M. & Siponen, M. 2015. An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset through Sanctioning Rhetoric.(Report). 39, 113.

Kraus, L., Wechsung, I. & Möller, S. 2017. Psychological Needs as Motivators for Security and Privacy Actions on Smartphones. *Journal of Information Security and Applications,* 34, 34-45.

Lavoie-Tremblay, M., Bonin, J.-P., Lesage, A. D., Bonneville-Roussy, A., Lavigne, G. L. & Laroche, D. 2010. Contribution of the Psychosocial Work Environment to Psychological Distress among Health Care Pofessionals before and During a Major Organizational Change.(Report). *The Health Care Manager,* 29**,** 293.

Lee, C., Lee, C. C. & Kim, S. 2016. Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity. *Computers & Security,* 59**,** 60-70.

Li, H., Sarathy, R., Zhang, J. & Luo, X. 2014. Exploring the Effects of Organizational Justice, Personal Ethics and Sanction on Internet Use Policy Compliance. *Information Systems Journal,* 24**,** 479-502.

Maddux, J. E. & Rogers, R. W. 1983. Protection Motivation and Self-Efficacy: A Revised Theory of Fear Appeals and Attitude Change. *Journal of Experimental Social Psychology,* 19**,** 469-479.

Moody, G. D. & Galletta, D. F. 2015. Lost in Cyberspace: The Impact of Information Scent and Time Constraints on Stress, Performance, and Attitudes Online. *Journal of Management Information Systems,* 32**,** 192-224.

Nunnally, J. & Bernstein, L. 1994. *Psychometric Theory,* New York, McGraw-Hill Higher, INC.

Pahnila, S., Siponen, M. & Mahmood, A. Employees' Behavior Towards Is Security Policy Compliance. System sciences, 2007. HICSS 2007. 40Th annual hawaii international conference on IEEE, 2007. 156b-156b.

Petter, S., Straub, D. & Rai, A. 2007. Specifying Formative Constructs in Is Research. *MIS Quarterly,* 31**,** 623-656.

Pham, H. C., El-Den, J. & Richardson, J. 2016. Stress-Based Security Compliance Model: An Exploratory Study. *Information and Computer Security,* 24**,** 326-347.

Pham, H. C., Pham, D. D., Brennan, L. & Richardson, J. 2017. Information Security and People: A Conundrum for Compliance. *Australasian Journal of Information Systems,* 21**,** 1-16.

Posey, C., Bennett, R. J. & Roberts, T. L. 2011a. Understanding the Mindset of the Abusive Insider: An Examination of Insiders' Causal Reasoning Following Internal Security Changes. *Computers & Security,* 30**,** 486–497.

Posey, C., Bennett, R. J., Roberts, T. L. & Lowry, P. B. 2011b. When Computer Monitoring Backfires: Privacy Invasions and Organizational Injustice as Precursors to Computer Abuse. *Journal of Information Systems Security,* 7**,** 24–47.

Posey, C., Roberts, T. L. & Lowry, P. B. 2015. The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems,* 32**,** 179-214.

Renaud, K. & Flowerday, S. 2017. Contemplating Human-Centred Security & Privacy Research: Suggesting Future Directions. *Journal of Information Security and Applications,* 34**,** 76-81.

Rhee, H. S., Kim, C. & Ryu, Y. U. 2009. Self-Efficacy in Information Security: Its Influence on End Users' Information Security Practice Behavior. *Computer & Security,* 28**,** 816-826.

Salanova, M., Grau, R. M., Cifre, E., &Llorens, S 2000. Computer Training, Frequency of Usage and Burnout: The Moderating Role of Computer Self- Efficacy. *Computers in Human Behavior,* 16**,** 575–590.

Salanova, M., Llorens, S. & Cifre, E. 2013. The Dark Side of Technologies: Technostress among Users of Information and Communication Technologies. *International Journal of Psychology,* 48**,** 422-436.

Schaufeli, W. B. & Bakker, A. B. 2004. Job Demands, Job Resources, and Their Relationship with Burnout and Engagement: A Multi-Sample Study. *Journal of Organizational Behavior,* 25**,** 293-315.

Schaufeli, W. B., Leiter, M. P., Maslach, C., & Jackson, S. E. 1996. Maslach Burnout Inventory-General Survey. In C. Maslach, S. E. Jackson, & M. P. Leiter (Eds.). *The Maslach Burnout Inventory: Test Manual* (3rd ed., pp. 22–26). Palo Alto, CA: Consulting Psychologists Press.

Schaufeli, W. B. & Taris, T. W. 2014. *A Critical Review of the Job Demands-Resources Model: Implications for Improving Work and Health*.

Schneier, B. 2008. *The Psychology of Security* (Online). http://www.schneier.com/essay-155.html. Available: http://www.schneier.com/essay-155.html (Accessed 20/7 2013).

Schrauf, R. W. & Navarro, E. 2005. Using Existing Tests and Scales in the Field. *Field Methods,* 17**,** 373-393.

Shih, S.-P., Jiang, J. J., Klein, G., & Wang, E. 2011. Learning Demand and Job Autonomy of It Personnel: Impact on Turnover Intention. *Computers in Human Behavior,* 27(6), pp. 2301-2307. doi:http://dx.doi.org/10.1016/j.chb.2011.07.009

Shu, Q., Tu, Q. & Wang, K. 2011. The Impact of Computer Self-Efficacy and Technology Dependence on Computer-Related Technostress: A Social Cognitive Theory Perspective. *International Journal of Human-Computer Interaction,* 27**,** 923-939.

Siponen, M., Mahmood, M. A. & Pahnila, S. 2014. Employee's Adherence to Information Security Policies: An Exploratory Field Study. *Information & Management,* 51**,** 217-224.

Steiger, J. H. 2007. Understanding the Limitations of Global Fit Assessment in Structural Equation Modeling. *Personality and Individual Differences,* 42**,** 893-898.

Toner, E., Haslam, N., Robinson, J. & Williams, P. 2012. Character Strengths and Wellbeing in Adolescence: Structure and Correlates of the Values in Action Inventory of Strengths for Children. *Personality and Individual Differences,* 52**,** 637-642.

Vacca, J. R. 2013. *Managing Information Security,* Burlington: Elsevier Science.

Vance, A. & Siponen, M. 2012. Is Security Policy Violations: A Rational Choice Perspective. *Journal of Organizational and End User Computing,* 24**,** 21-41.

Vance, A., Siponen, M. & Pahnila, S. 2012. Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory. *Information & Management,* 49**,** 190-198.

Von Solms, R. & Von Solms, B. 2004. From Policies to Culture. *Computer & Security,* 23**,** 275-279.

Wall, T. D., Jackson, P. R., Mullarkey, S., & Parker, S. K. (1996). The Demands-Control Model of Job Strain: A More Specific Test. *Journal of Occupational & Organizational Psychology,* 69(2), 153–166.

Warkentin, M., Shropshire, J. & Johnson, A. The It Security Adoption Conundrum: An Initial Step Towards Validation of Applicable Measures. Proceedings of the 13th Americas Conference on Information Systems, 2007 Keystone, CO.

Warkentin, M. & Willison, R. 2009. Behavioral and Policy Issues in Information Systems Security: The Insider Threat. *European Journal of Information Systems,* 18**,** 101-105.

Workman, M., Bommer, W. H., & Straub, D. 2008. Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test. *Computers in Human Behavior,* 24, 2799-2816.

Xanthopoulou, D., Bakker, A. B., Demerouti, E. & Schaufeli, W. B. 2007. The Role of Personal Resources in the Job Demands-Resources Model. *International Journal of Stress Management,* 14**,** 121-141.

Yuan, K. H. 2005. Fit Indices Versus Test Statistics. *Multivariate Behavioral Research,* 40**,** 115-148.